Human Factors in Cybersecurity, Vol. 208, 2026, 96–105
https://doi.org/10.54941/ahfe1007416

Micro-Decisions Under Time Pressure and Dark Patterns in Digital Interfaces

Dimitris Koutras[1], Kitty Kioskli[2], and Vangelis Malamas[1]

[1]Department of Informatics, University of Piraeus, 185 34 Piraeus, Greece
[2]trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands

ABSTRACT

Many risky actions are not caused by people deciding to do them, but by small mistakes that happen when we use digital technology every day. People often see permission dialogs, cookie banners, consent prompts and security warnings when they're not paying full attention and have a lot of other things going on in their minds. Research into cybersecurity has mostly looked at large-scale behaviours, like phishing response patterns or how people manage their passwords. But it has not looked at how short-term thinking affects people's ability to make good decisions about privacy and security. This theoretical work looks at how time pressure, cognitive fatigue, and interface manipulations ("dark patterns") create privacy issues that distort user judgment at the exact moment a security-relevant choice must be made. The paper looks at how small decisions are affected by limited attention, and when users don't have a lot of time, they often make quick decisions and rely on their instincts. When people are tired, they find it harder to tell the difference between safe and unsafe options. This research looks at how users behave when they are dealing with security prompts according to the related work. It also shows that privacy mistakes at a very small level can be seen as problems with how things are designed, rather than problems with motivation or education. This research makes it easier to understand privacy and permission errors as human-factors phenomena.

Keywords: Micro-decisions, Cognitive load, Dark patterns, Privacy decision-making

INTRODUCTION

Human error remains one of the most persistent challenges in cybersecurity. Despite all technical security measures, many security and privacy failures still comes from user actions and decisions. These actions are often described as "bad decisions" or a lack of awareness, that users knowingly choose unsafe options. However, in everyday digital environments, many risky actions do not result from deliberate choices. Instead, they arise from minor errors that occur when users interact with digital systems when they have limited time, attention and cognitive resources.

People now see lots of permission dialogs, cookie consent banners (Chen et al., 2023), privacy notices and security warnings. These prompts often appear while users are doing other things, like working, talking to people, or using the internet. When this happens, people are usually not thinking about

Received February 3, 2026; Revised March 29, 2026; Accepted April 14, 2026; Available online July 20, 2026

security. Instead of thinking carefully about what they need, users often just do what they need to do to get back to their original task. This means that people are less able to make good decisions about privacy and security when they are in a hurry, distracted, or tired. These conditions are known to make people make worse decisions and make more mistakes.

Research into cybersecurity has mostly looked at how users behave in general. Some common examples of these studies include how likely people are to fall for phishing attacks, how to create and reuse passwords, and people's long-term security habits. This work has given us some valuable insights, but it often treats user behaviour as a stable pattern that can be explained through knowledge, motivation, or individual differences. Research has not focused much on the small decisions that users make in the moment, especially when they are using interface elements that stop them from doing something else.

These short interactions can be understood as micro-decisions: small, time-bounded choices that are secondary to the user's main goal. Examples include deciding whether to allow an app to access location data, choosing between "accept all" and "manage settings" on a cookie banner, or dismissing a security warning in order to proceed. Individually, these decisions appear trivial. Collectively, however, they shape users' privacy exposure and security posture. Importantly, micro-decisions are often repeated, routine, and made with minimal conscious deliberation.

At the same time, interface design plays an important role in contributing how these decisions are perceived and executed. Many websites use design tricks to influence how users behave, sometimes on purpose. These tactics are also known as 'dark patterns'. They include techniques, like making the options look different, having default selections that can make you easy to share your data, or interaction flows that make it harder to make safer choices. When combined with time pressure and fatigue from thinking too much, these design choices can systematically make users more likely to make less secure choices. In these situations, errors should not be interpreted as irrational behavior, but as predictable responses to constrained cognitive conditions and manipulative interface designs.

Despite growing awareness of dark patterns and usable security, there is still a lack of integrated theoretical work that explains how short-term cognitive states interact with interface design at the exact moment a security-relevant decision is made. Privacy mistakes at this micro level are often framed as failures of user education or awareness. This framing overlooks the fact that many errors occur even when users understand security risks, simply because the context in which decisions are made makes careful evaluation difficult (Riaz et al., 2024).

This paper addresses this gap by surveying and synthesizing research from multiple domains, including human error theory, cognitive load and attention, decision-making under time pressure, human–computer interaction, and cybersecurity. We argue that privacy and security decisions should be treated as small, effortful tasks that compete for limited cognitive resources. When these tasks are embedded in interruptive

interfaces and influenced by dark patterns, they produce predictable patterns of error.

Background and Conceptual Foundations

Understanding why users make privacy- and security-relevant mistakes during everyday interactions requires moving beyond explanations based solely on knowledge or motivation. Instead, it calls for an examination of how human cognitive limitations, task context, and interface design interact at the moment a decision is made. This section reviews the fact that the problem is most relevant to micro-decisions under time pressure.

In everyday digital environments, users typically do not intend to compromise their privacy or security. Instead, errors emerge when routine actions are carried out automatically, without full conscious monitoring. From this perspective, many privacy and permission errors can be understood as execution failures rather than risk-taking.

According to (Ncubukezi et al., 2022) Ncubukezis's research the interfaces in the webpages often make the process more difficult by sending messages, interrupting the whole flow, and adding more duties. When users are focus on their main job that the platform offers, security and privacy warnings often appear. This means they have to stop what they're doing, switch contexts, and process this new information. These sudden changes make it harder for people to think about the results of their actions because they have to work harder. When given a choice of possibilities, people often choose the ones that seem important, familiar, or take little effort to save time. This behavior is not irrational, it is a normal reaction to cognitive constraints. To fully understand these minor opinions, you need to recognize that people often make choices that influence security when they are already close their own behavioral limitations.

According to (Tambe-Jagtap et al., 2023) Tambe-Jagtap's scope Human error is widely recognized as one of the dominant contributors to cybersecurity incidents, consistently emerging as a critical weakness even in systems with advanced technical protections. Prior work shows that many breaches originate not from sophisticated technical failures, but from everyday user actions such as falling for phishing messages, mismanaging passwords, or misconfiguring security settings. These errors are often described as negligence or lack of awareness. However, such interpretations overlook the cognitive and situational conditions under which users operate. Research adopting a human-centered perspective in Tambe-Jagtap et al. paper highlights that errors frequently occur when users are under stress or required to act quickly.

These issues are not uncommon, since they happen all the time when people interact with complicated systems in changing situations. Studies show that training and policy-based interventions alone don't always work in the long term, as users may keep making errors even if they know the best ways to do things. This collection of work supports the idea that human error in

cybersecurity should be seen as something that can be expected because of how people's brains work when they're using a system, rather than as users doing something wrong on purpose.

Fast vs Slow Thinking (Heuristics Under Pressure)

Prior work (Al-Hashem et al., 2023) emphasizes that cybersecurity is shaped not only by technical mechanisms but by how individuals "perceive and react to cyber dangers," noting that safe navigation of digital systems "depends on our ability to comprehend how individuals perceive and react to cyber dangers" . The authors highlight that cybersecurity decisions are influenced by "cognitive processes, emotions, and decision-making processes," and that these processes are "often influenced by psychological factors, biases, and heuristics" when individuals are "confronted with cyber risks".

The report emphasizes that decision-making in cybersecurity often transpires "under pressure," and that "human behaviours, perceptions, and decision-making processes are crucial in assessing the efficacy of cyber defences." It also says that cybersecurity solutions need to take into consideration "human cognitive limitations," because ignoring these aspects "creates vulnerabilities that are ripe for exploitation." This shows how important it is to make sure that security procedures match how people think and pay attention.

Now there is a very interesting perspective about a theory called "dual process" from Zhang et al. So, we have to take consider that two actors is this theory will be the users and the creator of the digital system. Research (Zhang et al., 2022) applying Dual Process Theory to cybersecurity contexts distinguishes between System-1 and System-2 modes of thinking, where System-1 thinking is based on fast, intuitive, autonomous responses which are often based on previous experience or heuristics, while System-2 thinking is based on slower, deliberate, and more analytical decision making. In BYOD environments, it is observed that with such a fast-paced lifestyle, employees must make snap judgments day to day, and that these decisions may be the chink hackers need to infiltrate companies. The study explicitly links human error to time-pressured contexts, stating that human error is the leading cause of data loss, particularly when users prioritize the completion of work over cyber security. Importantly, the results show that system-1 and system-2 thinking did not have significantly different results in phishing detection tasks, leading to the conclusion that new security measures focusing on both system-1 and system-2 thinking should be developed. This finding indicates that under realistic conditions of time pressure and routine interaction, both fast and slow cognitive processes remain vulnerable, reinforcing the need to design security mechanisms that account for heuristic-driven decisions rather than assuming sustained analytical reasoning.

The history behind this shows that we need to change how people and systems are responsible for security. There is a big effect on how people act when design choices make it harder to think or use automatic responses. This is because mistakes can be predicted based on known cognitive limits. From

this point of view, we can start to look at how interface design, such as the use of "dark patterns," works with people's flaws to create systemic privacy and security problems.

Micro-Decisions in Digital Interfaces

Concerning the micro-decisions users are asked over and over to confirm security warnings, allow or refuse permissions, accept or manage cookies, and move forward despite alerts. Each of these interactions seems small and low-risk on its own. But when you look at them all together, they make up a steady stream of choices that affect what data people share, which security features stay on, and how open systems become over time.

Three main things can be used to describe a micro-decision that affects security. First, it has a time limit. People are expected to answer fast, usually within a few seconds, so they can get back to what they were doing. Second, it gets in the way. The user is focused on something else when the choice pops up, like reading content, doing work, or talking to other people. Third, it's not seen as very important. Users don't usually see these prompts as times to think deeply because they happen so often and are common. Most importantly, micro-decisions happen over and over on different platforms and in different situations, making patterns of behaviour that become automatic. Users learn that reacting quickly lets them move forward and that pausing to think about each choice slows them down. Because of this, reactions become more and more automatic, based on recognition rather than logic.

Figure 1: Micro-decision under time pressure.

In the field of cybersecurity, bad judgment is typically thought to be the main reason for cyber incidents, and people's negligent acts are often blamed for them. People who think this way typically believe that when things get tough, they need to use mental shortcuts and simple rules. Instead of using these shortcuts, you should think carefully. The authors, (Schaltegger et al., 2024) on the other hand, believe that heuristics are techniques of making decisions that leave out certain information so that you may reach a conclusion faster than more time-consuming and difficult methods like analytical reasoning. People say that heuristics are flexible, cost-effective, and able to work with little information and short deadlines when there is ambiguity. There is little or no knowledge about cybersecurity, the chances of attacks are unknown, and the ways people attack are always evolving. The research argues that heuristic decision-making is particularly advantageous in these contexts, as straightforward heuristics enable individuals to make rapid decisions based on little information, rather than engaging in complex and time-intensive analysis.

Table 1: Micro-decisions vs traditional security decisions.

Dimension	Micro-Decisions	Traditional Security Decisions
Duration	Seconds	Minutes or longer
Context	Interruptive	Deliberate
Cognitive state	Fatigue / distraction	Focused
Processing mode	Heuristic	Analytical
Design influence	High	Moderate
Error type	Error type	Error type

Users of information technologies are often presented with complex decisions and utilize multiple cognitive processes to arrive at an action, particularly when responding to computer security notifications. When presented with a decision about whether to proceed to a website or return to a safer page, a user may weigh their options and consider the context that they find themselves in, but they may also simply ignore the message, perhaps because these messages have become mundane. Prior research highlights that much of the past work has concerned users' habituation to notifications and the impact of emotional factors on responses to security messages (Conrad et al., 2022).

The research by Conrad et al. shows that cybersecurity alerts cause emotional reactions. This suggests that people process their emotions to some extent when they see security alerts. These findings suggest that responses to security warnings are not solely analytical; rather, they are influenced by affective reactions that arise during brief, interruptive interactions. This supports the notion that security-related decisions are frequently made as minor, transient choices within the context of ongoing activities.

Dark Patterns and Interface Manipulation

Micro-decisions don't happen in a space that is neutral. The way alternatives are shown, emphasized, delayed, or concealed in the interface affects how they look. (Trzaskowski et al., 2023) Even while users are typically expected to make quick decisions on privacy and security, the design of many digital interfaces actively pushes these decisions in certain directions. People often call these practices "dark patterns." They are design methods for interfaces that change how people engage by taking advantage of cognitive limits, habitual responses, and differences in attention.

Dark patterns don't usually make people do things that aren't safe when it comes to privacy and security. Instead, they discreetly make it more likely that users will choose options that are good for the system, service provider, or data collector, especially when they are under pressure or distracted. This impact works best since it works on small decisions (Nie et al., 2024).

Dark patterns work because they fit with how people already act when they have limited cognitive resources. When people don't have a lot of time to think about their options, they employ visual clues, defaults, and perceived effort to help them make choices. Interface designs that make these cues

stand out too much can systematically prejudice decisions without needing to lie in the usual way.

For instance, letting one option stand out visually while putting the others in smaller type or on separate screens takes use of the fact that people tend to choose the most obvious option. In the same way, showing the fastest way ahead as the least privacy-protecting choice takes advantage of users' desire to avoid interruptions. In these cases, consumers are not deceived about the presence of alternatives; instead, the interface makes some choices simpler to think about and others harder (Kollmer et al., 2023).

In the context of information systems, user autonomy can be defined as self-governance that leads to independent choices and the expression of free will among users (Kollmer et al., 2023). Dark patterns deceive and manipulate users using elements of the choice architecture, defined as the structure and presentation of choices, and through the exploitation of psychological vulnerabilities. Organizations utilize dark patterns to increase their revenue, collect data, and steer users' attention, often by influencing how options are composed, highlighted, or made accessible.

A recurring mechanism is the asymmetry of effort between choices, where one option is facilitated while others are complicated or obstructed, leading users to favor choices that require less cognitive and interactional effort. Such manipulation techniques provide complete and accurate options and information to the user but exploit users' psychological vulnerabilities and prevent informed choices through composition and complication. In addition, dark patterns may introduce excessive or unjustified hurdles that complicate users' task completion, increasing cognitive load and encouraging users to abandon reflective decision-making in favor of faster, more automatic responses.

Dark Patterns as Systematic Manipulation of Micro-Decisions

Dark patterns are designed to change people's behaviour by taking advantage of psychological flaws and attention spans, rather than by taking away choices or giving false information. In digital interfaces, this is done through choice design, which is how options are put together, highlighted, or made hard to get to. Because of this, users are often formally free to choose, but in practice are pushed toward outcomes that are good for the service provider (Nie et al., 2024).

At the level of micro-decisions, this kind of trickery works especially well. People often have to make privacy and security decisions during short, interruptive exchanges where they have to think quickly and with few mental resources (Schäfer et al., 2024). Users don't do reflective evaluation at these times; instead, they focus on perceptual cues and minimizing effort. On the other hand, dark designs take advantage of this by making one choice easy and quick while other choices are hard, take longer, or are hidden behind extra steps. This imbalance can stop people from making good decisions even when all of their options are correct and available. It does this by making it harder to think and connect at the exact moment when a choice needs to be made.

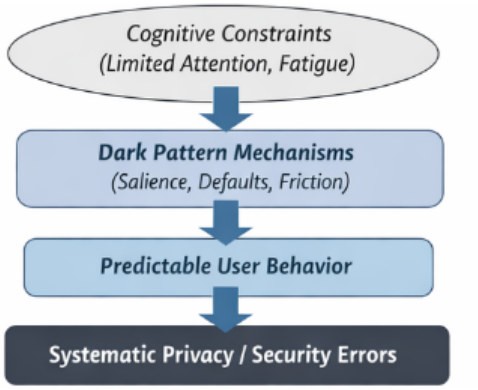

Figure 2: Dark patterns as design-induced error.

One important way that dark patterns work is by taking advantage of people's limited attention. A lot of the time, interfaces ask users to make decisions when they are already thinking about something else. When this happens, designs that stress speed, visual dominance, or default ways make users want to fix the problem as soon as possible. Over time, users become used to the same patterns of interactions and stop seeing these prompts as important choices. Instead, they see them as normal problems that need to be solved. At this point, interaction is automated, and small choices are replaced by predictable behaviors based on past experiences instead of conscious choice (Schäfer et al., 2024).

It is important to note that dark patterns have effects that go beyond how individuals connect with each other. These designs set long-term user habits and standards by making certain interaction flows normal. People figure out which options are "easy," "annoying," and not worth the trouble (Nie et al., 2024). This gradual training takes away freedom not by forcing it, but by making it harder to do things on your own and wearing you out mentally. From this point of view, privacy and security mistakes should be seen as results of bad design rather than mistakes made by individuals. Users are not acting irrationally, they are just getting good at using interfaces that encourage speed and discourage thought.

Table 1: Sample human systems integration test parameters (Folds et al., 2008).

Access to Amenities	Illumination Conditions
Acoustics	Maintenance/installation safety
Atmosphere (temperature, pressure, humidity, quality, etc.)	Maintenance/installation time to complete

CONCLUSION

This paper set out to examine a class of security and privacy decisions that are often overlooked precisely because they appear small. Rather than focusing on large-scale user behaviors or long-term security practices, we examined what happens at the exact moment a user is interrupted by a prompt, banner, or warning and is required to decide quickly. Across the literature surveyed,

a consistent pattern emerges, many privacy and security failures do not stem from ignorance or deliberate risk-taking, but from the interaction between human cognitive limitations and the way digital interfaces structure choice.

When the user's main task isn't making decisions, they rely on rapid, heuristic-based answers that prioritize speed over critical thought. This activity doesn't make sense. It's a response that has changed over time to work in settings that necessitate rapidity, frequent changes in context, and few breaks.

Interface design plays a critical role in amplifying these effects. Dark patterns exploit known cognitive constraints by introducing asymmetries of effort, visual dominance, and default paths that cause less secure outcomes. At the level of micro-decisions, these design choices do not need to deceive users explicitly. Instead, they work by aligning with users' desire to resolve interruptions quickly and return to their main activity. Training, awareness campaigns (Koutras et al., 2024), and policy reminders assume that users can consistently engage in slow, analytical reasoning at every decision point. The literature reviewed here suggests that this assumption is unrealistic in everyday digital contexts. Even knowledgeable and motivated users are vulnerable when decisions are embedded in interruptive, time-pressured interactions.

This point of view has big effects on both design and study. For researchers, this shows that they need to do more detailed studies that record how people make decisions in real time. These studies could include controlled experiments, logging of real interactions in real time, and methods based on simulations. It means that designers and system builders may be better off reducing cognitive friction, making sure that choices require the same amount of work, and respecting users' limited attention than adding more information. So, making systems safer doesn't just mean asking people to think more; it also means making systems that don't need constant attention to stay safe.

Understanding how small choices are made in the real world gives us a more realistic way to deal with mistakes made by people in cybersecurity. This work helps move the focus from users to designers when it comes to privacy and security. It does this by recognizing cognitive limits and looking at how interfaces affect behavior at key times.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided for the following projects: the 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411.

REFERENCES

Al-Hashem, N., & Saidi, A. (2023). The psychological aspect of cybersecurity: understanding cyber threat perception and decision-making. *International Journal of Applied Machine Learning and Computational Intelligence, 13*(8), 11–22.

Chen, S., McCracken, J., Lu, K., Wang, T., & Hou, T. (2023, October). Taking a Look into the Cookie Jar: *A* Comprehensive Study towards the Security of Web Cookies. In *Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing* (pp. 474–479).

Conrad, C. D., Aziz, J. R., Henneberry, J. M., & Newman, A. J. (2022). Do emotions influence safe browsing? Toward an electroencephalography marker of affective responses to cybersecurity notifications. *Frontiers in neuroscience, 16,* 922960

Kollmer, T., & Eckhardt, A. (2023). Dark patterns. *Business & information systems engineering, 65*(2), 201–208.

Koutras, D., Kioskli, K., & Kotzanikolaou, P. (2024). The Human Factor Impact on a Supply Chain Tracking Service Through a Risk Assessment Methodology. *Human Factors in Cybersecurity,* 198.

Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. In *Proceedings of the 17th International Conference on Information Warfare and Security* (p. 395).

Nie, L., Zhao, Y., Li, C., Luo, X., & Liu, Y. (2024). Shadows in the interface: A comprehensive study on dark patterns. *Proceedings of the ACM on Software Engineering, 1*(FSE), 204–225.

Riaz, R., Vasconcelos, A., & Pinto, P. (2024, October). An overview of user psychological manipulation techniques in ui/ux web design. In *2024 Cyber Awareness and Research Symposium* (CARS) (pp. 1–6). IEEE.

Schaltegger, T., Ambuehl, B., Ackermann, K. A., & Ebert, N. (2024). Re-thinking decision-making in cybersecurity: Leveraging cognitive heuristics in situations of uncertainty.

Schäfer, R., Sahabi, S., Brocker, A., & Borchers, J. (2024, October). Growing up with dark patterns: How children perceive malicious user interface designs. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction* (pp. 1–17).

Tambe-Jagtap, S. N. (2023). Human-Centric Cybersecurity: Understanding and Mitigating the Role of Human Error in Cyber Incidents. *SHIFRA, 2023,* 53–59.

Trzaskowski, J. *(2023)*. Persuasion, manipulation, choice architecture and dark patterns. In *Research Handbook on EU Internet Law* (pp. 309–330). Edward Elgar Publishing.t

Zhang, R., Bello, A., & Foster, J. L. (2022, October). BYOD security: using dual process theory to adapt effective security habits in BYOD. In *Proceedings of the Future Technologies Conference* (pp. 372–386). Cham: Springer International Publishing.